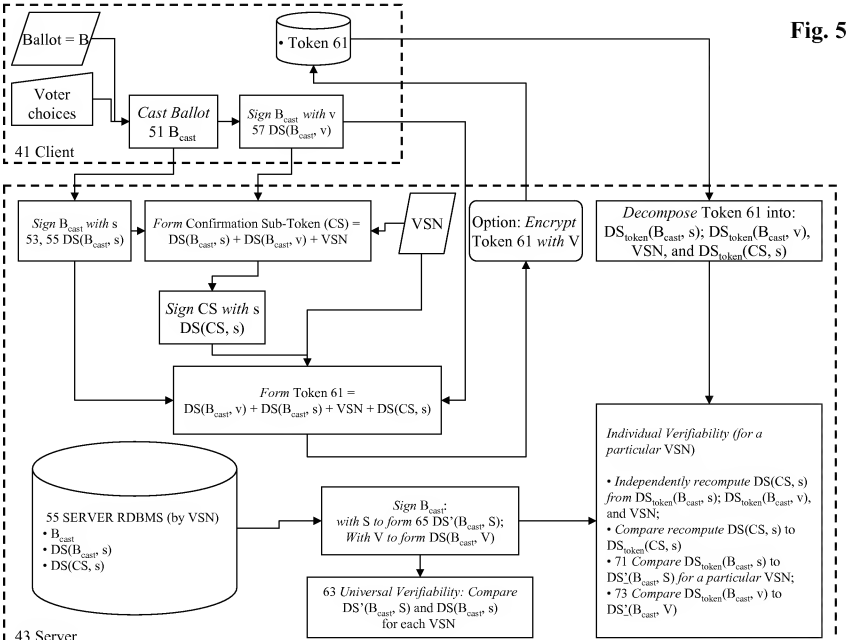
Fig. 5


Ballot = B
Voter choices
41 Client
• Token 61
Cast Ballot
51 B cast
Sign B cast with v
57 DS(B cast, v)
Sign B cast with s
53, 55 DS(B cast, s)
Form Confirmation Sub-Token (CS) =
DS(B cast, s) + DS(B cast, v) + VSN
VSN
Option: Encrypt
Token 61 with V
Decompose Token 61 into:
DS token(B cast, s); DS token(B cast, v),
VSN, and DS token(CS, s)
Sign CS with s
DS(CS, s)
Form Token 61 =
DS(B cast, v) + DS(B cast, s) + VSN + DS(CS, s)
55 SERVER RDBMS (by VSN)
• B cast
• DS(B cast, s)
• DS(CS, s)
Sign B cast:
with S to form 65 DS'(B cast, S);
With V to form DS(B cast, V)
63 Universal Verifiability: Compare
DS'(B cast, S) and DS(B cast, s)
for each VSN
Individual Verifiability (for a particular VSN)
• Independently recompute DS(CS, s) from DS token(B cast, s); DS token(B cast, v), and VSN;
• Compare recompute DS(CS, s) to DS token(CS, s)
• 71 Compare DS token(B cast, s) to DS'(B cast, S) for a particular VSN;
• 73 Compare DS token(B cast, v) to DS'(B cast, V)
43 Server